

DOCKET NO.: 211526US2PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Marc GIRAULT, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/FR00/00174

INTERNATIONAL FILING DATE: January 26, 2000

FOR: AUTHENTICATION OR SIGNATURE PROCESS WITH A REDUCED CALCULATIONS SET

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
France	99/00887	27 January 1999

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. **PCT/FR00/00174**. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Surinder Sachar

Marvin J. Spivak
Attorney of Record
Registration No. 24,913
Surinder Sachar
Registration No. 34,423



22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 1/97)

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

09 / 889557

R E P U B L I Q U E F R A N C

PCT/FR 00/00174

FR00/174



EJU

REC'D 04 FEB 2000

WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

DOCUMENT DE PRIORITÉ

COPIE OFFICIELLE

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA RÈGLE
17.1.a) OU b)

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

24 JAN. 2000

Fait à Paris, le

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE

26 bis, rue de Saint Petersbourg
75800 PARIS Cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

THIS PAGE BLANK (USPTO)



26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa
N° 55-1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES

27/01/99

N° D'ENREGISTREMENT NATIONAL

99 00887 -

DÉPARTEMENT DE DÉPÔT

71

DATE DE DÉPÔT

27 JAN. 1999

2 DEMANDE Nature du titre de propriété industrielle

- brevet d'invention demande divisionnaire
 certificat d'utilité transformation d'une demande de brevet européen

demande initiale

brevet d'invention

différé

immédiat

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

SOCIETE DE PROTECTION
DES INVENTIONS

3, rue du Docteur Lancereaux
75008 PARIS

n°du puuoor permanent références du correspondant SP 16207.C/RS 01 53 83 94 0
C.03072

téléphone

date

Établissement du rapport de recherche

certificat d'utilité n°

Titre de l'invention (200 caractères maximum)

oui

non

PROCEDE D'AUTHENTIFICATION OU DE SIGNATURE A NOMBRE DE CALCULS REDUIT.

3 DEMANDEUR (S) n° SIREN

code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

Forme juridique

FRANCE TELECOM

Société Anonyme

Nationalité (s) Française

Adresse (s) complète (s)

6 Place d'Alleray 75015 PARIS

Pays

France

En cas d'insuffisance de place, poursuivre sur papier libre

4 INVENTEUR (S) Les inventeurs sont les demandeurs

oui

non

Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES

requise pour la 1ère fois

requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTIÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

D. DU BOISBAUDRIN
CPI 950 304

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cedex 08 SP 16207 C/R S
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL

990087

TITRE DE L'INVENTION :

PROCEDE D'AUTHENTIFICATION OU DE SIGNATURE A NOMBRE DE CALCULS REDUIT.

LE(S) SOUSSIGNÉ(S)

D. DU BOISBAUDRY
c/o SOCIETE DE PROTECTION DES INVENTIONS
25 rue de Ponthieu
75008 PARIS

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

GIRAULT Marc

9 rue Bernard Vanier
14000 CAEN

PAILLES Jean-Claude

4 rue des Loisirs
14610 EPRON

FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire
PARIS LE 27 JANVIER 1999

D. DU BOISBAUDRY
CPI 950 304

DOCUMENT COMPORTANT DES MODIFICATIONS

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du Code de la Propriété Intellectuelle, est signalé par la mention "R.M." (revendications modifiées)

**PROCEDE D'AUTHENTIFICATION OU DE SIGNATURE A NOMBRE DE
CALCULS REDUIT**

Domaine technique

5 La présente invention a pour objet un procédé d'authentification ou de signature à nombre de calculs réduit.

L'invention concerne plus précisément le domaine de la cryptographie dite à clé publique. Dans 10 de tels procédés, l'entité à authentifier possède une clé secrète et une clé publique associée. L'entité authentifierante a uniquement besoin de cette clé publique pour réaliser l'authentification.

L'invention concerne plus précisément encore le 15 domaine des procédés d'authentification dits à connaissance nulle ou sans apport de connaissance ("zero-knowledge"). Dans ce type de procédé, l'authentification se déroule suivant un protocole qui, de façon prouvée, et sous des hypothèses reconnues 20 comme parfaitement raisonnables par la communauté scientifique, ne révèle rien sur la clé secrète de l'entité à authentifier.

Plus précisément encore, l'invention concerne des procédés sans apport de connaissance basés sur le 25 problème de la factorisation (c'est-à-dire sur la difficulté de décomposer de grands entiers en un produit de nombres premiers).

L'invention trouve une application dans tous les systèmes nécessitant d'authentifier des entités ou 30 des messages, ou de signer des messages, et plus particulièrement dans les systèmes où le nombre de calculs effectués par l'entité authentifierée constitue un paramètre critique. C'est notamment le cas des

cartes à microcircuit standards ou à bas coût, non pourvues d'un coprocesseur arithmétique (appelé souvent cryptoprocesseur) pour accélérer les calculs cryptographiques.

5 Une application typique de l'invention est le porte-monnaie électronique, qui requiert un très haut niveau de sécurité, tout en excluant l'usage d'un cryptoprocesseur, soit pour des raisons de coût, soit pour des raisons techniques (par exemple l'utilisation 10 d'une interface sans contact), soit pour les deux.

15 Une autre application possible est la télécarte de future génération, pour laquelle les contraintes de coût sont encore bien plus sévères que pour le porte-monnaie électronique.

15

Etat de la technique antérieure

De nombreux protocoles d'identification du type sans apport de connaissance sont connus. On peut citer, par exemple :

- 20 - le protocole de FIAT-SHAMIR décrit dans l'article de A. FIAT et A. SHAMIR intitulé "How to prove yourself : Practical solutions to identification and signature problems", publié dans "Advances in Cryptology : Proceedings of CRYPTO'86, Lecture Notes in Computer Science", vol. 263, Springer-Verlag, Berlin, 1987, pp. 186-194,
- 25 - le protocole de GUILLOU-QUISQUATER décrit dans l'article de L.C. GUILLOU et J.J. QUISQUATER, intitulé "A practical zero-knowledge protocole fitted 30 to security microprocessors minimizing both transmission and memory", publié dans "Advances in Cryptology : Proceedings of EUROCRYPT'88, Lecture

Notes in Computer Science", vol. 330, Springer-verlag, Berlin, 1988, pp. 123-128,

- le protocole de GIRAUT décrit dans la demande de brevet français FR-A-2 716 058, basé sur le problème dit du logarithme discret.

De façon générale, la plupart des protocoles d'identification (ou d'authentification de message) à apport nul de connaissance se déroulent en trois échanges. On supposera, afin de simplifier la description, que l'entité authentifiante B connaît déjà tous les paramètres publics caractéristiques de l'entité à authentifier A, à savoir son identité, sa clé publique, etc..

Lors du premier échange, A fournit à B une valeur c dite "engagement", image par une fonction pseudo-aléatoire h d'un paramètre x (lui-même calculé à partir d'un nombre r choisi au hasard par A), ainsi que, s'il y a lieu, du message à authentifier ou à signer : $c=h(x,[M])$ où la notation $[M]$ exprime que M est optionnel. C'est la première étape. Dans certains protocoles, il peut y avoir plusieurs engagements.

Lors d'un deuxième échange, B envoie à A un paramètre e choisi au hasard (la "question"). C'est la deuxième étape.

Lors du troisième échange, A fournit à B une "réponse" y , cohérente avec la question e , l'engagement c et la clé secrète v de A (troisième étape).

Enfin, B contrôle la réponse reçue. Plus précisément, B recalcule x à partir des éléments y , e et v par $x=\phi(y,e,v)$; puis il vérifie que : $c=h(\phi(v,e,y),[M])$ (quatrième étape).

Dans le cas où il n'y a pas de message à authentifier, le recours à la fonction pseudo-aléatoire

h est optionnel. On peut prendre alors $c=x$. La vérification consiste alors à vérifier que $x=\phi(y, e, v)$.

Dans certains protocoles, il y a un ou deux échanges supplémentaires entre les entités à authentifier et authentifiante.

Dans le cas d'une signature de message, les deux premiers échanges sont supprimés, car le paramètre e est choisi égal à c ; A calcule alors successivement, et seul, c, $e(=c)$ et y.

Le nombre u de questions possibles est directement relié au niveau de sécurité du protocole. Ce dernier est défini comme la probabilité p de détection d'un imposteur (c'est-à-dire d'une entité C qui tente frauduleusement de se faire passer pour A), et est caractérisé par un paramètre k. Les nombres p et k sont reliés par l'égalité : $p=1-2^{-k}$. En d'autres termes, l'imposteur n'a qu'une chance sur 2^k de réussir son imposture. Dans le cas présent, on peut montrer que, si le protocole repose sur un problème mathématique difficile, et si les engagements sont de longueur suffisante, alors il suffit que la longueur de u soit égale à k bits. Typiquement, k est égal à 32 bits, ce qui donne seulement une chance sur quatre milliards de réussir une imposture. Dans les applications où l'échec d'une identification peut avoir des conséquences très néfastes (poursuite judiciaire par exemple), cette longueur peut être réduite à quelques bits.

Dans les protocoles basés sur la factorisation, le calcul de x à partir de r, ou le calcul de y à partir de e, ou les deux, implique(nt) des opérations modulo n où n est un nombre composé difficile à factoriser. Ce nombre est de type universel, c'est-à-

dire généré par une tierce partie de confiance, mémorisé et utilisé par toutes les entités qui y sont rattachées. Le caractère universel de n implique qu'il est de très grande taille (typiquement 1024 bits), car
5 la découverte de la factorisation de n compromettrait les clés secrètes de tous les utilisateurs.

Dans leur version de base, aucun des protocoles mentionnés plus haut ne peut être mis en oeuvre dans une application soumise à de fortes contraintes, (bas 10 coût, faible complexité) telles que décrites dans la section précédente, car les calculs requis ne pourraient être effectués par une carte à microcircuit qui ne serait pas dotée d'un cryptoprocesseur.

La demande de brevet français FR-A-2 752 122 15 décrit bien une optimisation de ces protocoles, mais cette optimisation reste limitée aux protocoles basés sur le logarithme discret dans un mode dit "à précalculs" qui présente l'inconvénient d'impliquer des rechargements à intervalles réguliers.
20

La présente invention a justement pour but de remédier à cet inconvénient. Elle tend à réduire le nombre de calculs effectués par l'entité authentifiée dans les protocoles d'identification (ou 25 d'authentification de message ou de signature de message) sans apport de connaissance basés sur la factorisation, cette réduction pouvant atteindre un facteur 2 ou 3.

Elle rend ainsi possible, et plus 30 particulièrement quand on la couple avec le protocole Guillou-Quisquater, l'exécution rapide d'un algorithme d'identification (ou d'authentification de message ou de signature de message) à clé publique dans une carte

à microcircuit standard à bas coût, pour des applications telles que le porte-monnaie électronique ou la télécarte de future génération.

5 Exposé de l'invention

Ce but est atteint en choisissant pour le module n non pas un paramètre de type universel, mais un paramètre de type individuel (en d'autres termes, chaque utilisateur possède sa propre valeur de n), et 10 d'exploiter ce choix des deux manières suivantes, (qui peuvent d'ailleurs être avantageusement combinées) :

- 1) d'abord en choisissant une taille de n inférieure à la valeur usuelle (typiquement inférieure à 1000 et par exemple comprise entre 700 et 800) ; cela est 15 possible car la découverte de la factorisation de n ne compromet plus que la clé secrète de l'utilisateur correspondant et en aucune façon celle des autres ; cette seule modification permet de réduire déjà d'environ 40% la durée des calculs 20 effectués modulo n ;
- 2) si l'utilisateur a conservé les facteurs premiers de n dans la mémoire de son dispositif de sécurité, on peut mettre en oeuvre la technique dite des restes chinois, pour réduire encore d'environ 40% la durée 25 des calculs effectués modulo n, lorsque le nombre de facteurs premiers est 2 ; cette réduction peut être encore amplifiée en utilisant plusieurs facteurs premiers (typiquement 3 ou 4).

Au total, on peut donc réduire les temps de 30 calcul modulo n d'au moins 60%, c'est-à-dire d'au moins un facteur 2.

De façon précise, l'invention a pour objet un procédé d'authentification mettant en œuvre une première entité dite "à authentifier", possédant une clé publique v et une clé secrète s, ces clés étant reliées par une opération modulo n où n est un entier appelé module, et une seconde entité dite "authentifiante", connaissant la clé publique v, ce procédé comprenant des échanges d'informations du type à apport nul de connaissance entre l'entité à authentifier et l'entité authentifiante et des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo n, ce procédé étant caractérisé en ce que le module n est propre à l'entité à authentifier, laquelle communique ce module à l'entité authentifiante.

Dans un mode de mise en œuvre avantageux, l'opération modulo n est du type $v=s^t \pmod{n}$ où t est un paramètre, et les échanges d'informations du type à apport nul de connaissance et les calculs cryptographiques sont les suivants :

- l'entité à authentifier choisit au hasard un (des) nombre(s) entier(s) r compris entre 1 et n-1 et calcule un (des) paramètre(s) x égal (égaux) à $rt \pmod{n}$, puis un (des) nombre(s) c appelé(s) engagement(s) qui est (sont) une (des) fonction(s) de ce (ces) paramètre(s) et éventuellement d'un message (M), et envoie cet (ces) engagement(s) à l'entité authentifiante ;
- l'entité authentifiante reçoit le ou les engagement(s) c, choisit au hasard un nombre e appelé "question" et envoie cette question à l'entité à authentifier ;

- l'entité à authentifier reçoit la question e, effectue un (des) calcul(s) utilisant cette question e et la clé secrète s, le résultat de ce (ces) calcul(s) constituant une (des) réponse(s) y, et envoie cette (ces) réponse(s) à l'entité authentifiante ;
- l'entité authentifiante reçoit la (les) réponse(s) y, effectue un calcul utilisant la clé publique v et le module n, et vérifie par une opération modulo n que le résultat de ce calcul est bien cohérent avec le (les) engagement(s) reçu(s).

La présente invention a également pour objet un procédé de signature de message par une entité dite "signataire", cette entité possédant une clé publique v et une clé secrète s, ces clés étant reliées par $v=s^{-t} \pmod{n}$ où n est un entier appelé "module" et t un paramètre, procédé dans lequel l'entité signataire calcule un engagement c fonction notamment du message à signer et un nombre y fonction de la clé secrète, émet les nombres y et c qui constituent la signature du message et le message, ce procédé étant caractérisé en ce que le module n est propre au signataire.

Dans un mode de mise en œuvre avantageux, le signataire choisit au hasard un nombre entier r compris entre 1 et n-1, calcule un paramètre x égal à $r^t \pmod{n}$, calcule un nombre c fonction du paramètre x et du message à signer, calcule un nombre y à l'aide de sa clé secrète s et fonction des nombres r et e, et émet les nombres c et y comme signature.

Description détaillée de modes particuliers de mise en oeuvre de l'invention

Dans la description qui suit, l'invention est supposée être appliquée au protocole GUILLOU-QUISQUATER
5 mais, naturellement, il ne s'agit là que d'un exemple et l'invention n'est nullement limitée à ce protocole.

On rappelle que dans le protocole de GUILLOU-
QUISQUATER, les paramètres universels sont le module n ,
produits de nombres premiers et comprenant au moins
10 1024 bits, et un nombre t entier.

La clé publique v et la clé secrète s sont reliées par l'équation : $v=s^{-1}(\text{mod } n)$.

Le niveau de sécurité choisi est u (inférieur ou égal à t , et le plus souvent, $u=t$).

15 L'authentification de A par B, que l'on peut appeler respectivement Alice et Bob selon la terminologie en usage, se déroule comme suit :

1. Alice choisit r dans l'intervalle $[1, n-1]$, calcule $x=r^t(\text{mod } n)$ puis $c=h(x, [M])$ et envoie c à Bob.
- 20 2. Bob choisit e dans l'intervalle $[0, u-1]$ et envoie e à Alice.
3. Alice calcule $y=rs^e(\text{mod } n)$ et envoie y à Bob.
4. Bob calcule $x=y^t v^e(\text{mod } n)$ et vérifie que $c=h(x, [M])$

25 Dans le cas où il n'y a pas de message à authentifier, le recours à la fonction pseudo-aléatoire h est optionnel : on peut prendre $c=x$. La vérification consiste alors à vérifier que $x=y^t v^e(\text{mod } n)$.

Avec le protocole modifié selon l'invention, le seul paramètre universel est t_0 .

30 La clé publique est (n, v) , où n a au moins 768 bits. La clé publique v et la clé secrète s d'Alice sont reliées par l'équation : $v=s^{-1}(\text{mod } n)$.

La clé secrète peut aussi inclure les facteurs premiers de n afin de bénéficier du deuxième volet de l'invention.

Le paramètre t peut être inclus dans la clé 5 publique (dans ce cas, il n'y a plus de paramètre universel).

Le niveau de sécurité choisi par Alice et Bob est u (inférieur ou égal à t ; souvent $u=t$).

L'authentification d'Alice par Bob se déroule 10 comme décrit plus haut, mais avec des calculs plus rapides grâce à un module plus petit.

Puisque tous les calculs d'Alice sont effectués modulo n , le facteur de gain obtenu sur une unique multiplication modulaire se répercute sur l'ensemble 15 des calculs effectués par Alice durant l'exécution du protocole. Il en serait de même avec les protocoles de Fiat-Shamir ou de Girault par exemple (dans ce dernier cas, il n'y a pas de gain dans l'étape 3 puisqu'il n'y a plus de calculs modulaires, mais de toute façon le 20 temps d'exécution de cette étape est négligeable par rapport à l'exponentiation modulaire de la première étape).

L'invention peut également être mise en oeuvre 25 par la technique dite des restes chinois, qui consiste à effectuer les calculs modulo chacun des nombres premiers composant n . Comme ces nombres sont nécessairement beaucoup plus petits, ces calculs sont rapides. Il reste à calculer le résultat modulo n à 30 l'aide d'une opération dite de reconstitution. Cette technique est décrite dans l'article de J.J QUISQUATER et C. COUVREUR, intitulé "Fast decipherment algorithm for RSA public-key cryptosystem", publié dans

"Electronic Letters", vol. 18, Octobre 1982, pp. 905-907.

On considère donc le cas où n est le produit de deux facteurs premiers p et q .

5 D'après le théorème de Bezout, il existe deux entiers a et b tels que $ap+bq=1$.

Pour calculer $y=x^e \pmod{n}$, on commence par "réduire" x modulo chacun des nombres premiers en calculant $x_p=x \pmod{p}$ et $x_q=x \pmod{q}$. On réduit 10 également e modulo $(p-1)$ et $(q-1)$ en calculant $e_p=\text{emod}(p-1)$ et $e_q=\text{emod}(q-1)$. (Dans le protocole de Guillou-Quisquater, e est toujours inférieur à $p-1$ et $q-1$ et par conséquent $e_p=e_q=e$).

On calcule alors $y_p=x_p^{e_p} \pmod{p}$ et
 15 $y_q=x_q^{e_q} \pmod{q}$. Quand p et q sont de tailles semblables, chacun de ces calculs est environ 8 fois plus rapide que le calcul $y=x^e \pmod{n}$ quand la taille de e est celle de n (premier cas) ; 4 fois plus rapide quand elle est inférieure ou égale à celle de p
 20 (deuxième cas comme par exemple dans l'algorithme). L'ensemble des deux calculs est donc, soit 4 fois plus rapide, soit 2 fois plus rapide.

Il reste à reconstituer y à partir de y_p et y_q , ce qui est réalisé par l'opération :

$$25 \quad y=y_p+ap(y_q-y_p) \pmod{n}$$

Au total, la méthode des restes chinois permet d'accélérer le calcul d'un facteur compris entre 3 et 4 dans le premier cas, entre 1,5 et 2 dans le deuxième cas. Lorsque le nombre de facteurs premiers (supposés 30 de tailles semblables) est égal à k , le facteur

d'accélération est proche de k^2 dans le premier cas,
proche de k dans le deuxième cas.

REVENDICATIONS

1. Procédé d'authentification mettant en oeuvre une première entité dite "à authentifier" (A), possédant une clé publique v et une clé secrète s, ces clés étant reliées par une opération modulo n où n est un entier appelé module, et une seconde entité dite "authentifiante" (B), connaissant la clé publique v, ce procédé comprenant des échanges d'informations du type à apport nul de connaissance entre l'entité à authentifier (A) et l'entité authentifiante (B) et des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo n, ce procédé étant caractérisé en ce que le module n est propre à l'entité à authentifier (A), laquelle communique ce module à l'entité authentifiante (B).

2. Procédé selon la revendication 1, dans lequel l'opération modulo n est du type $v=s^t \pmod{n}$, t étant un paramètre et les échanges d'informations du type à apport nul de connaissance et les calculs cryptographiques sont les suivants :

- l'entité à authentifier (A) choisit au hasard un (des) nombre(s) entier(s) r compris entre 1 et $n-1$ et calcule un (des) paramètre(s) (x) égal (égaux) à $r^t \pmod{n}$, puis un (des) nombre(s) c appelé(s) engagement(s) qui est (sont) une (des) fonction(s) de ce (ces) paramètre(s) et éventuellement d'un message (M), et envoie cet (ces) engagement(s) à l'entité authentifiante (B) ;
- l'entité authentifiante (B) reçoit le ou les engagement(s) c, choisit au hasard un nombre e

appelé "question" et envoie cette question à l'entité à authentifier (A) ;

- l'entité à authentifier (A) reçoit la question e, effectue un (des) calcul(s) utilisant cette question e et la clé secrète s, le résultat de ce (ces) calcul(s) constituant une (des) réponse(s) y, et envoie cette (ces) réponse(s) à l'entité authentifiante (B) ;
- l'entité authentifiante (B) reçoit la (les) réponse(s) y, effectue un calcul utilisant la clé publique v et le module n, et vérifie par une opération modulo n que le résultat de ce calcul est bien cohérent avec le (les) engagement(s) reçu(s).

15

3. Procédé selon la revendication 2, dans lequel le nombre n est inférieur à 1 000.

20 4. Procédé selon la revendication 3, dans lequel le nombre n est compris entre 700 et 800.

25 5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel n est le produit de deux nombres entiers (p, q) et dans lequel les opérations modulo n sont effectuées par la méthode dite "des restes chinois".

30 6. Procédé de signature de message par une entité dite "signataire" (A), cette entité possédant une clé publique v et une clé secrète s, ces clés étant reliées par $v=s^{-t} \pmod{n}$ où n est un entier appelé "module" et t un paramètre, procédé dans lequel l'entité signataire (A) calcule un engagement c fonction notamment du

message à signer M et un nombre y fonction de la clé secrète, émet les nombres y et c qui constituent la signature du message M et le message M , ce procédé étant caractérisé en ce que le module n est propre au signataire.

7. Procédé de signature de message selon la revendication 6, dans lequel le signataire choisit au hasard un nombre entier r compris entre 1 et $n-1$, calcule un paramètre x égal à $r^t \pmod n$, calcule un nombre c fonction du paramètre x et du message à signer M , calcule un nombre y à l'aide de sa clé secrète s et fonction des nombres r et e , et émet les nombres c et y comme signature.

REVENDICATIONS

1. Procédé d'authentification mettant en oeuvre une première entité dite "à authentifier" (A), possédant une clé publique v et une clé secrète s, ces clés étant reliées par une opération modulo n où n est un entier appelé module, et une seconde entité dite "authentifiante" (B), connaissant la clé publique v, ces entités, telles que cartes à microcircuit, porte-monnaie électronique, télécarte, comprenant des moyens aptes à échanger des informations du type à apport nul de connaissance et à effectuer des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo n, ce procédé étant caractérisé en ce que le module n est propre à l'entité à authentifier (A), laquelle communique ce module à l'entité authentifiante (B).

2. Procédé selon la revendication 1, dans lequel l'opération modulo n est du type $v=s^{-t} \pmod{n}$, t étant un paramètre et les échanges d'informations du type à apport nul de connaissance et les calculs cryptographiques sont les suivants :

- l'entité à authentifier (A) choisit au hasard un (des) nombre(s) entier(s) r compris entre 1 et n-1 et calcule un (des) paramètre(s) (x) égal (égaux) à $r^t \pmod{n}$, puis un (des) nombre(s) c appelé(s) engagement(s) qui est (sont) une (des) fonction(s) de ce (ces) paramètre(s) et éventuellement d'un message

(M), et envoie cet (ces) engagement(s) à l'entité authentifiante (B) ;

- l'entité authentifiante (B) reçoit le ou les engagement(s) c, choisit au hasard un nombre e appelé "question" et envoie cette question à l'entité à authentifier (A) ;
- l'entité à authentifier (A) reçoit la question e, effectue un (des) calcul(s) utilisant cette question e et la clé secrète s, le résultat de ce (ces) calcul(s) constituant une (des) réponse(s) y, et envoie cette (ces) réponse(s) à l'entité authentifiante (B) ;
- l'entité authentifiante (B) reçoit la (les) réponse(s) y, effectue un calcul utilisant la clé publique y et le module n, et vérifie par une opération modulo n que le résultat de ce calcul est bien cohérent avec le (les) engagement(s) reçu(s).

20 3. Procédé selon la revendication 2, dans lequel le nombre n est inférieur à 1 000.

25 4. Procédé selon la revendication 3, dans lequel le nombre n est compris entre 700 et 800.

30 5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel n est le produit de deux nombres entiers (p, q) et dans lequel les opérations modulo n sont effectuées par la méthode dite "des restes chinois".

6. Procédé de signature de message par une entité dite "signataire" (A), cette entité possédant une clé publique v et une clé secrète s, ces clés étant reliées par $v=s^{-t} \pmod n$ où n est un entier appelé "module" et t un paramètre, ce signataire, tel que carte à microcircuit, porte-monnaie électronique, télécarte, comprenant des moyens aptes à calculer un engagement c fonction notamment du message à signer M et un nombre y fonction de la clé secrète, à émettre les nombres y et c qui constituent la signature du message M et le message M, ce procédé étant caractérisé en ce que le module n est propre au signataire.

7. Procédé de signature de message selon la revendication 6, dans lequel le signataire choisit au hasard un nombre entier r compris entre 1 et n-1, calcule un paramètre x égal à $r^t \pmod n$, calcule un nombre c fonction du paramètre x et du message à signer M, calcule un nombre y à l'aide de sa clé secrète s et fonction des nombres r et e, et émet les nombres c et y comme signature.

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)